

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

BONNIE HERMANN, individually, and on
behalf of all others similarly situated.,

Plaintiff,

v.

RUSH STREET GAMING LLC and
SUGARHOUSE HSP GAMING, L.P. d/b/a
RIVERS CASINO PHILADELPHIA,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Bonnie Hermann (“Plaintiff”), individually and on behalf of all others similarly situated (collectively, “Class Members”), brings this Class Action Complaint against Defendants Defendants Rush Street Gaming LLC and Defendants Sugarhouse HSP Gaming, L.P. d/b/a Rivers Casino Philadelphia (collectively, “Defendants”), and alleges upon personal knowledge as to herself and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard her other similarly situated individuals’ (“Class Members”) personally identifiable information (“PII”).

2. Defendants are or operate a casino and entertainment development located in the Fishtown neighborhood of Philadelphia.

3. On or around November 18, 2024, Defendants learned by way of an investigation that an unauthorized third-party accessed their computer systems and stole Plaintiff's and Class Members PII (the "Data Breach").¹

4. Defendants acknowledged that "an unauthorized actor accessed and/or took certain files stored on [their] computer servers."²

5. According to Defendants, the PII that was compromised included Plaintiff's and Class Members' names and "one or more of the following: Social Security number, and/or bank account information used for direct deposit."³

6. Defendants began mailing written notice of the Data Breach on or about December 30, 2024.

7. As set forth below, the Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect client's PII from the foreseeable threat of a cyberattack.

8. The security of Plaintiff's and Class Members' identities is now at risk because of Defendants' wrongful conduct as the PII that Defendants collected and maintained is now in the hands of data thieves. Given the type of data involved – including Social Security numbers – this present risk will continue for the course of their lives.

9. Plaintiff, on behalf of herself and the putative class she seeks to represent, asserts claims for (i) negligence, (ii) breach of express contract, and (iii) breach of implied contract. Plaintiff and Class Members thus seek actual damages, statutory damages, restitution, injunctive and declaratory relief (including significant improvements to Defendants' data security protocols

¹ See Data Breach Notice Letter ("Notice Letter"), <https://ago.vermont.gov/document/2024-12-30-rivers-casino-philadelphia-data-breach-notice-consumers> (last visited Jan. 9, 2025).

² *Id.*

³ *Id.*

and employee training practices), reasonable attorneys' fees, costs, expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

JURISDICTION AND VENUE

11. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendants, there are more than 100 Members of the Class, and the aggregate amount in controversy exceeds \$5,000,000 exclusive of interests and costs.

12. This Court has personal jurisdiction over Defendants because Defendants maintains their principal place of business in Philadelphia, Pennsylvania and conducts substantial business in Pennsylvania and in this district through their principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because Defendants resides in this district, and this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

PARTIES

14. Plaintiff Bonnie Hermann at all relevant times was and is a resident and citizen of the Commonwealth of Pennsylvania.

15. Plaintiff Bonnie Hermann was a consumer of Rivers Casino Philadelphia using the website platform. Plaintiff Hermann provided her PII as a condition of participating in services and receiving payouts.

16. At the time of the Data Breach, Defendant retained Plaintiff Hermann's PII in its system.

17. Plaintiff Hermann is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

18. Plaintiff received a letter dated December 30, 2024 notifying her that her PII was compromised in the Data Breach discovered on or around November 18, 2024. Specifically, Plaintiff received a notice indicating that her name, social security number, and bank account information were impacted by the Data Breach.

19. Upon information and belief, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties in the Data Breach.

20. Plaintiff Hermann suffered actual injury from having Plaintiff's Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to Plaintiff's Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

21. As a direct and proximate result of the Data Breach, and in addition to the injuries alleged above, Plaintiff Hermann also experienced actual fraud, including a fraudulent attempt in around early January 2025 to secure a loan through a loan provider using Plaintiff's PII without

Plaintiff's express consent. Plaintiff additionally received a notice through CreditWise that identified a line of credit opened using Plaintiff Hermann's PII that was reported on December 19, 2024, as well as an alert of a credit inquiry on January 1, 2025, all occurring without authorization from Plaintiff. Additionally, Plaintiff experienced unauthorized charges to her virtual Apple Card for \$63.67 on January 8, 2025. Plaintiff has likewise seen a voluminous increase in spam phone calls and messages resulting in undue attention addressing these spam attempts.

22. As a result of the Data Breach, Plaintiff Hermann has made reasonable efforts to mitigate the impact of the Data Breach, including monitoring Plaintiff's accounts for additional fraudulent activity. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

23. As a result of the Data Breach, Plaintiff is at a present and continued increased risk of identity theft and fraud for years to come.

24. Plaintiff Hermann plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

25. Plaintiff Hermann suffers emotional stress from the public release of her PII and anxiety regarding the potential harm from this release.

26. Defendant Rush Street Gaming LLC is a limited liability company registered in the State of Delaware, and upon information and belief, is headquartered in Illinois.

27. Defendant Sugarhouse HSP Gaming, L.P. d/b/a Rivers Casino Philadelphia is a Delaware Limited Partnership with their principal place of business located at 1001 North Delaware Avenue, Philadelphia, Pennsylvania 19123.

FACTUAL ALLEGATIONS

I. The Data Breach

16. On or around December 30, 2024, Defendants publicly announced that confidential PII maintained by Defendants was accessed by an unauthorized party.

17. Defendants began notifying only certain affected persons of the Data Breach by U.S. mail on December 30, 2024.

18. According to the Notice Letter, Defendants discovered on November 18, 2024, that an unauthorized party gained access to Defendants' systems. Defendants confirmed that "an unauthorized actor accessed and/or took certain files stored on [their] computer systems" that contained individual's PII.

19. The PII that was compromised included Plaintiff's and Class Members' names and "one or more of the following: Social Security number, and/or bank account information used for direct deposit."

20. According to UK security firm Sophos, "[c]yberattackers on average have 11 days after breaching a target network before they're being detected...and often when they are spotted it's because they've deployed ransomware." Sophos found that this was "more than enough time for an attacker to get a thorough overview of what a target network looks like, where their weaknesses lie, and for ransomware attackers to wreck it."

21. To put in context, according to Sophos, "11 days potentially provide attackers with approximately 264 hours for malicious activity, such as lateral movement, reconnaissance, credential dumping, data exfiltration, and more. Considering that some of these activities can take

just minutes or a few hours to implement, 11 days provide attackers with plenty of time to do damage.”

II. Defendants Obtain, Collect, and Store Plaintiff’s and Class Members’ PII

24. Defendants are a casino entertainment development based in Philadelphia, Pennsylvania. Defendants offer gaming, dining, and other forms of entertainment.

25. In the regular course of their business, Defendants collect highly private PII from their employees for employment purposes and customers and other individuals who interact or otherwise transact with Defendants for business purposes. Defendants store this highly sensitive information digitally.

26. On information and belief, Plaintiff and Class Members provided personal information to Defendants exchange for employment or gaming and other entertainment services.

27. Defendants were obligated, as an employer and vendor that collects sensitive consumer data, to protect that information.

22. Defendants are in complete operation, control, and supervision of their servers and systems.

23. Defendants intentionally configured and designed their servers and systems in such a way that allowed it to be susceptible to cyberattack. Further, Defendants intentionally configured and designed their servers and systems without adequate data security protections and without regard to Plaintiff’s and Class Members’ PII, which was disclosed to cybercriminals.

24. By obtaining, using, disclosing, and deriving a benefit from Plaintiff’s and Class Members’ PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff’s and Class Members’ PII from disclosure.

25. Plaintiff and Class Members reasonably expect that employers and vendors, such as Defendants, will use the utmost care to keep their PII confidential and securely maintained, to use this information for business purposes only, to only store it until it is no longer needed, to properly dispose of it, and to make only authorized disclosures of this information.

26. Defendants failed to prioritize data and cybersecurity by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiff's and Class Members' PII.

27. Had Defendants remedied the security deficiencies, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendants would have prevented the theft of Plaintiff's and Class Members' confidential PII.

28. Given the rise in cyberattacks on companies that store a high-volume of individuals sensitive PII, Defendants knew or should have known that they were prime targets for this Data Breach.

III. Defendants' Data Security Failures

29. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection." However, Defendants took no such precautions to appropriately secure Plaintiff's and Class Members' PII.

30. Further, Defendants' data retention practices were also woefully lacking. Defendants continued to store and maintain PII for many years after Defendants had appropriate use for such data.

31. Defendants failed to archive such PII and remove it from their servers and systems, which allowed hackers to gain access to the PII in the Data Breach.

32. Up to, and including, the period when the Data Breach occurred, Defendants breached their duties, obligations, and promises to Plaintiff and Class Members by their failure to:

- a. hire qualified personnel and maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;
- b. properly supervise and train their employees, and ensure that their vendor's employees were supervised and trained, about the risk of cyberattacks and how to mitigate them, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques, what to do if they suspect such attacks, and how to prevent them;
- c. address well-known warnings that their systems and servers, and those of their vendors, were susceptible to a data breach;
- d. implement certain protocols that would have prevented unauthorized programs, such as malware and ransomware, from being installed on their servers and systems that accessed customers' personal information and otherwise would have protected customers' sensitive personal information;
- e. install software to adequately track access to their network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented customers' sensitive personal information from being stolen. Specifically, there are recommended, available measures to prevent data from leaving protected systems and being sent to untrusted networks outside of the corporate systems; and
- f. adequately safeguard customers' sensitive personal information and maintain an adequate data security environment to reduce the risk of a data breach or unauthorized disclosure.

33. Up to, and including, the period when the Data Breach occurred, Defendants breached their duties, obligations, and promises to Plaintiff and Class Members by their failure to oversee the entrustment of Plaintiff's and Class Members' PII.

IV. Defendants' Failure to Comply with Government and Industry Guidelines, Standards, and Recommendations

34. Industry experts identify several best practices, that at a minimum, should be implemented by ARM companies such as Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

35. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls ("CIS CSC"), which are all established standards in reasonable cybersecurity readiness.

36. The above government and industry frameworks are existing and applicable industry standards in the financial services industry. Defendants failed to comply with these accepted standards.

37. At all times, Defendants were in complete control of the configuration and design of their servers and systems.

V. Defendants' Data Security Failures Constitute Unfair and Deceptive Practices and Violations of Consumers' Privacy Rights

38. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce."

The U.S. Federal Trade Commission (“FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for sensitive personal information is an “unfair practice” in violation of the FTC Act.

39. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

40. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal information that they keep, properly dispose of personal information that is no longer needed; encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone may be trying to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

41. The FTC has also published a document entitled “FTC Facts for Business,” which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

42. The FTC further recommends companies not maintain PII longer than is needed for authorization of a transaction, limit access to private data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has also brought enforcement actions against businesses for failing to adequately and reasonably protect personal data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to sensitive personal information as an unfair act or practice prohibited by Section 5 of the FTC Act. The FTC has issued orders against businesses that have failed to employ reasonable measures to secure sensitive personal information. These orders provide further guidance to businesses regarding their data security obligations.

44. The FTC deems the failure to employ reasonable and appropriate measures to protect against unauthorized access to sensitive personal information an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

45. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to PII or to prevent the disclosure of such information to unauthorized individuals, as reflected by the sensitive driver's license numbers and Social Security numbers stolen, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

46. Defendants were always fully aware of their obligations to protect PII since it was in the business as an ARM of obtaining, collecting, and disclosing PII as well as collecting, storing, and using other confidential personal and financial information. Defendants were also aware of the significant repercussions that would result from their failure to do so.

47. Prior to the Data Breach and during the breach itself, Defendants failed to follow guidelines set forth by the FTC and actively mishandled the management of their IT security.

48. Furthermore, by failing to have reasonable data security measures in place, Defendants engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

VI. The Value of the Disclosed PII and Effects of Unauthorized Disclosure

49. The fact that Defendants has a privacy policy shows that it understood the protected PII it transfers, acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.⁴

50. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cyber criminals routinely post stolen personal information on anonymous websites, making the information widely available to the criminal underworld.

51. There is an active and robust market for this information. As John Sancenito, President of Information Network Associates, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

52. Some of the forms of PII involved in this Data Breach are particularly concerning. Unique Social Security and driver's license numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies, in order to update the person's accounts with those entities.

⁴ [https://www.riverscasino.com/philadelphia/privacy-policy#:~:text=The%20types%20of%20information%20we,\)%2C%20employment%20informati on%20\(such%20as \(last visited Jan. 7, 2025\)\).](https://www.riverscasino.com/philadelphia/privacy-policy#:~:text=The%20types%20of%20information%20we,)%2C%20employment%20informati on%20(such%20as (last visited Jan. 7, 2025)).)

53. Experian, a globally recognized credit reporting agency, has explained “[n]ext to your Social Security number, your driver’s license number is one of the most important pieces of information to keep safe from thieves.” This is because a driver’s license number is connected to an individual’s vehicle registration, insurance policies, records on file with the Department of Motor Vehicles, and other government agencies, financial institutions, places of employment, doctor’s offices, and other entities.

54. For these reasons, driver’s license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person’s name.

55. ***Social Security numbers***—which were also compromised as a result of the Data Breach—are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive and cannot easily be replaced.

56. Indeed, even the Social Security Administration (“SSA”) warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security Number, you should not be able to use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

57. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often Social Security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cyber criminals and a particularly attractive form of PII to steal and then sell.

58. The ramifications of Defendants’ failure to keep Plaintiff’ and Class Members’ PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the “dark web” may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

59. Thus, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if their servers and systems were breached. However, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

60. As highly sophisticated parties that handle sensitive PII, Defendants failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to

ensure the security and confidentiality of Plaintiff⁷ and other Class Members' PII to protect against anticipated threats of intrusion of such information.

61. Identity thieves use stolen PII for various types of criminal activities, such as when personal and financial information is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud, and government fraud.

62. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are other ways for cyber criminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

63. There is often a lag time between when fraud occurs versus when it is discovered and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

64. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

65. Plaintiff and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

66. Thus, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

VII. The Data Breach Damaged Plaintiff and Class Members

67. As a result of Defendants' deficient security measures, Plaintiff and Class Members have been harmed by the compromise of their sensitive personal information, which is likely currently for sale on the dark web and through private sale to other cyber criminals and/or being used by criminals for identify theft and other fraud-related crimes.

68. Plaintiff and Class Members face a substantial and imminent risk of fraud and identity theft as their names have now been linked with their driver's license and Social Security numbers, email addresses, and addresses as a result of the Data Breach. These specific types of information are associated with a high risk of fraud.

69. Many Class Members will also incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

70. Plaintiff and Class Members also suffered a "loss of value" of their sensitive personal information when it was stolen by hackers in the Data Breach. A robust market exists for stolen personal information. Hackers sell personal information on the dark web—an underground market for illicit activity, including the purchase of hacked personal information—at specific identifiable prices. This market serves as a means to determine the loss of value to Plaintiff and Class Members.

71. Plaintiff's and Class Members' stolen personal information is a valuable commodity to identity thieves. William P. Barr, former United States Attorney General, made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal information is to use it to defraud

consumers or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit payment card fraud. One commentator confirmed, explaining that, “[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud.”

72. Identity thieves can also combine data stolen in the Data Breach with other information about Plaintiff and Class Members gathered from underground sources, public sources, or even Plaintiff’s and Class Members’ social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiff and Class Members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiff’s and Class Members’ names, taking out loans in Plaintiff’s and Class Members’ names, using Plaintiff’s and Class Members’ information to obtain government benefits, filing fraudulent tax returns using Plaintiff’s and Class Members’ information, obtaining Social Security numbers in Plaintiff’s and Class Members’ names but with another person’s photograph, and giving false information to police during an arrest.

73. Plaintiff and Class Members have spent and will continue to spend substantial amounts of time monitoring their accounts for identity theft and fraud, the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming, especially because Defendants have failed to disclose how long the Data Breach lasted, forcing customers to continue to monitor their accounts indefinitely.

74. Class Members who experience actual identity theft and fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to fraudulent charges. To the extent Class Members are charged

monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class Members will be harmed further by the loss of rewards points or airline mileage that they cannot accrue while awaiting replacement cards. The inability to use payment cards may also result in missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

75. In the case of a data breach, merely reimbursing a consumer for a financial loss due to identity theft or fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

76. A victim whose personal information has been stolen or compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose personal information (including driver's license and Social Security numbers) has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

77. To date, Defendants have done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendants have only offered one year of inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

78. The one year of credit monitoring offered to persons whose PII was compromised is wholly inadequate, as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What is more, Defendants place the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

79. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches to various individuals rather than in bulk to a single buyer. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

CLASS ALLEGATIONS

80. Plaintiff brings this class action on behalf of herself and all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. The proposed Class is defined as:

All persons whose PII was compromised in the Data Breach detected by Defendants on or about November 18, 2024.

81. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

82. Numerosity: The Members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. Upon information and belief, Plaintiff believes the proposed Class includes thousands of individuals who have been damaged by

Defendants' conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendants' records.

83. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

- a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII from unauthorized access and disclosure;
- b. Whether Defendants' actions and their lax data security practices used to protect Plaintiff's and Class Members' PII violated the FTC Act, and/or other state laws and/or Defendants' other duties discussed herein;
- c. Whether Defendants failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;
- d. Whether Plaintiff and Class Members suffered injury as a proximate result of Defendants' negligent actions or failures to act;
- e. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII;
- f. Whether an implied contract existed between Class Members and Defendants providing that Defendants would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;
- g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and Class Members;

- h. Whether Defendants' actions and inactions alleged herein constitute gross negligence;
- i. Whether Defendants breached their duties to protect Plaintiff's and Class Members' PII; and
- j. Whether Plaintiff and all other Members of the Class are entitled to damages and the measure of such damages and relief.

84. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of themselves and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

85. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed Members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

86. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class in that they have no interests adverse to, or conflict with, the Class they seek to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

87. Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class Members are relatively small compared to the burden and expense that

would be required to individually litigate their claims against Defendants, so it would be impracticable for Class Members to individually seek redress from Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I NEGLIGENCE

(On Behalf of Plaintiff and the Class)

88. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

89. Defendants owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in their possession, custody, or control. Defendants' duty arose independently from any contract to protect Plaintiff's and Class Members' PII.

90. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

91. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of Defendants' inadequate security measures. By receiving, maintaining, and handling Plaintiff's and Class Members' PII that is routinely targeted by criminals for unauthorized access, Defendants was obligated to act with reasonable care to protect against these foreseeable threats.

92. Defendants' duty also arose from Defendants' position as a business associate. Defendants hold themselves out as a trusted business associate of their clients, and thereby assume a duty to reasonably protect the PII it obtains from their clients. Indeed, Defendants, who receive, maintain, and handle the PII from their employees and customers were in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

93. Defendants knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' PII and the importance of maintaining secure systems. Defendants knew, or should have known, of the many data breaches that targeted financial institutions in recent years.

94. Given the nature of Defendants' business, the sensitivity and value of the PII they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

95. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class Members' PII.

96. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would

result in the unauthorized release, disclosure, destruction and/or dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

97. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

98. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the imminent and certainly impending increased risks of medical identity theft they face and will continue to face; (vi) actual or attempted fraud; (vii) continued risk of exposure to hackers and thieves of their Personal Information which remains in Defendants' possession, custody, and control; and (viii) emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks.

COUNT II
BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiffs and the Class)

99. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

100. Defendants' Privacy Policy created an express contractual obligation to safeguard and protect the sensitive information of Plaintiff and Class Members.

101. The Privacy Policy also contractually promised that Defendants would only share Plaintiff's and Class Members' PII to certain authorized recipients in only a limited set of circumstances.

102. Defendants breached both of these contractual duties by failing to adequately safeguard Plaintiff's and Class Members' PII, and by allowing it to be disseminated to unauthorized third parties.

103. Plaintiffs and class members substantially performed their part of the bargain.

104. Defendants' breach of these contractual obligations in the Privacy Policy and elsewhere caused damages to Plaintiffs and class members, as set forth herein.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

105. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

106. Plaintiff and Class Members were required to provide Defendants with their PII in exchange for employment and/or use of Defendants' services.

107. By Plaintiff and Class Members providing their PII, and by Defendants accepting this PII, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that: (1) Defendants would adequately safeguard Plaintiff's and Class Members' PII from foreseeable threats; (2) Defendants would only disclose the PII to authorized individuals for business purposes; (3) Defendants would delete the PII of Plaintiff and

Class Members once it no longer had a legitimate need; and (4) Defendants would provide Plaintiff and Class Members with notice within a reasonable amount of time after suffering a data breach.

108. Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards when they entered into the implied contracts with Defendants.

109. Defendants provided consideration by providing employment and/or their services, while Plaintiff and Class Members provided consideration by providing valuable property, their PII. Defendants benefitted from the receipt of this PII by receiving their labor and/or services as employees, and/or by increasing profit from additional business.

110. Plaintiff and the Class Members fully performed their obligations under the implied contracts with Defendants.

111. Plaintiff and Class Members would not have provided their PII to Defendants in the absence of Defendants' implied promise to keep their PII reasonably secure.

112. Defendants breached their implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures.

113. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and Class Members sustained damages, as alleged above. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages, in an amount to be proven at trial.

114. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for their lifetime.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in her favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, nominal damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and


F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: January 9, 2025

Respectfully submitted,



Benjamin F. Johns (PA ID 201373)

Samantha E. Holbrook (PA ID 311829)

Andrea L. Bonner (PA ID 332945)

SHUB & JOHNS LLC

Four Tower Bridge

200 Barr Harbor Drive, Suite 400

Conshohocken, PA 19428

Phone: (610) 477-8380

bjohns@shublawayers.com

sholbrook@shublawayers.com

abonner@shublawayers.com

Counsel for Plaintiff and the Putative Class